STUDENT COMPUTER AND INTERNET USE RULES

All students are responsible for their actions and activities involving school unit computers, network and Internet services, and for their computer files, passwords and accounts. The use of school computing devices, networks and other infrastructure by students is a privilege, not a right. These rules provide general guidance concerning the use of the school unit's computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by students. Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator or information technology director. These rules apply to all school computing devices (see definition for computer in policy IJNDB) and all school-provided laptops wherever used, and all uses of school servers, Internet access and networks regardless of how they are accessed.

A. Acceptable Use

1. The school unit's computers, network and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum and instructional goals.

2. Students must comply with all Board policies, school rules and expectations concerning student conduct and communications when using school computers and network whether on or off school property.

3. Students also must comply with all specific instructions from school staff and volunteers when using the school unit's computers and must read and sign an acceptable use policy.

B. Prohibited Uses

Unacceptable uses of school unit computers include, but are not limited to, the following:

1. **Accessing or Communicating Inappropriate Materials –** Students may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

2. **Illegal Activities and Digital Citizenship –** Students must practice good digital citizenship and may not use the school unit's computers, network and Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. The school unit assumes no responsibility for illegal activities of students while using school computers.

3. **Violating Copyrights or Software Licenses –** Students may not copy, download or share any type of copyrighted materials (including music or films) without the owner's permission; or copy or download software without the express authorization of the information technology director. Unauthorized copying of software or other copyrighted material such as movies, etc. is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for copyright or licensing violations by students.

4. **Plagiarism –** Students may not represent as their own work any materials obtained on the Internet (such as term papers, articles, music, etc). When Internet sources are used in student work, the author, publisher and web site must be identified.

5. **Use for Non-School-Related Purposes -** Using the school unit's computers, network and Internet services for any personal reasons not connected with the educational program, authorized after-school activities or school assignments.

6. **Misuse of Passwords/Unauthorized Access –** Students may not share passwords; use other users' passwords; access or use other users' accounts; or attempt to circumvent network security systems.

7. **Malicious Use/Vandalism –** Students may not engage in any malicious use, disruption or harm to the school unit's computing devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses. Students shall take every precaution to ensure that the computing devices are protected and safe from damage, including liquid spills, drops, etc.

8. **Avoiding School Filters –** Students may not attempt to or use any software, utilities, proxy servers, peer-to-peer networks or other means to access Internet sites or content blocked by the school filters. Students may not bypass school networks by broadcasting a personal network device from a cell phone or other personal device.

9. **Unauthorized Access to Blogs/Social Networking Sites, Etc. –**Students may not access blogs, social networking sites, etc. to which student access is prohibited by filters or other means. Occasionally access to such sites or tools may be permissible when authorized by a teacher or administrator for educational purposes.

11. **Mass Email –** Students must not send mass email or SPAM from a school unit computing device or network.

12. **Inventory Asset Tags -** Students are not permitted to remove or deface asset tags from computing devices.

C. Compensation for Losses, Costs and/or Damages

The student and his/her parents are responsible for compensating the school unit for any losses, costs or damages incurred for violations of Board policies/procures and school rules while the student is using school unit computing devices or network, including the cost of investigating such violations. The school unit assumes no responsibility for any unauthorized charges or costs incurred by a student while using school unit computers or network.

D. Student Security

A student is not allowed to reveal his/her full name, address, telephone number, social security number or other personal information on the Internet while using a school computer without prior permission from a teacher. Students should never agree to meet people they have contacted through the Internet without parental permission. Students should inform their teacher if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

E. System Security

The security of the school unit's computers, network and Internet services is a high priority. Any student who identifies a security problem must notify his/her teacher or building administrator immediately. The student shall not demonstrate the problem to others or access unauthorized material.

F. Additional Rules for Computing Devices Issued to Students

1. Computing devices are loaned to students as an educational tool and may be used for purposes specifically authorized by school staff and the MLTI program.

2. Parents are encouraged to attend an informational meeting before a laptop will be issued to their child. Both the student and his/her parent must sign the school's acknowledgment form and acceptable use policy.

3. Students and their families are responsible for the proper care of district computing devices at all times, whether on or off school property, including costs associated with repairing or replacing the laptop. RSU#2 offers a protection plan for parents to cover replacement costs and/or repair costs for damages not covered by the laptop warranty. Parents who choose not to purchase the protection plan should be aware that they are responsible for any costs associated with loss, theft or damage to a laptop issued to their child.

4. A laptop that is, or suspected to be, lost or stolen must be reported to the building administrator or IT department immediately. If a laptop is stolen, a report shall be made to the local police and the DOE (if required) immediately.

5. The Board's policy and rules concerning computer and Internet use apply to use of laptops or district-owned computing devices at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of computing devices issued by school staff.

6. Violation of policies or rules governing the use of computers, or any careless use or vandalism of a computing device may result in a student's device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies/procedures or school rules.

7. Students will provide the laptop login password to their parents. Parents are responsible for supervising their child's use of the laptop and Internet access when in use at home and away from school.

8. The laptop may only be used by the student to whom it is assigned and his or her parents to the extent permitted by the MLTI program.

9. All use of school-loaned laptops by all persons must comply with the school's Student Computer Use Policy and Rules and Acceptable Use Policy.

10. Computing devices must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

G. Additional Rules for Use of Privately-Owned Computing Devices by Students

1. A student's privately-owned computing device, cell phone, etc. in school must adhere to all Student Computer Use Policies and Rules and the Acceptable Use Policy. There must be an educational basis for the use of any computing device brought from home.

2. The Technology Director or staff will determine whether a student's privately-owned computing device meets the school unit's network requirements and will determine if that device may be used in the school buildings.

3. Use of these devices may be prohibited if it is determined that there is not a suitable educational basis and/or if the demands on the school unit's network or staff would be unreasonable.

4. The student is responsible for proper care and security of his/her privately-owned computing device, including any costs of repair, replacement or any modifications needed to use the computer at school.

5. The school unit is not responsible for damage, loss or theft of any privately-owned devices.

6. Students are required to comply with all Board policies, administrative procedures and school rules while using privately-owned computing devices at school.

7. Students have no expectation of privacy in their use of a privately-owned computing device while at school. The school unit reserves the right to search a student's privately-owned device if there is reasonable suspicion that the student has violated Board policies, administrative procedures or school rules, or engaged in other misconduct while using the device.

.

8. Violation of any Board policies, administrative procedures or school rules involving a student's privately-owned computing device may result in the revocation of the privilege of using the device at school and/or disciplinary action.

9. The school unit may confiscate any privately-owned computing device used by a student in school without authorization as required by these rules. The contents of the device may be searched in accordance with applicable laws and policies.

Cross Reference: IJNDB – Student Computer and Internet Use

First Reading: 4/6/11
Adopted: 5/4/11